Security
in Mobile Ad Hoc Networks

Source: Rudi Belotti, Frank Lyner

Contents

- Basic introduction to ad hoc networks
- Basic Mechanisms
  - Routing
  - Physical location
- Security Mechanism
  - Public Key infrastructure
  - Key establishment
- Optimized Link State Routing (OLSR)
  - Security Problems
  - Reputation-based Scheme (joint work with JP Vilela)

Introduction

- Definition of Mobile Ad Hoc Network
  - Collection of mobile nodes that can dynamically form a network that does not rely on any infrastructure.
- Characteristics of the nodes
  - Wireless
  - Limited power and CPU resources

Characteristics and Constraints

- Limited Range
  - Due to limited power supplies
  - Each node acts also as router to relay packets

    COLLABORATION
- Mobility
  - Nodes can dynamically join and leave the network
  - Routing information only valid for limited time.
- No (centralized) public key infrastructure

Security Goals

- Availability
  - Very challenging due to all characteristics
- Confidentiality, Integrity, Authentication
  - Usually require a public key infrastructure
  - Security mechanisms must be distributed

Basic Mechanisms

- Basic Mechanism
  - Services and/or guarantees that would usually be provided by the infrastructure
- Major Security Goal: Availability
  - Nearly all attacks are DoS attacks
  - Even more difficult to handle than in “normal” networks due to collaboration requirement, mobility and nature of communication channel

Physical

- Threat of capture and compromise
  - Most scenarios of ad hoc networks include nodes without surveillance
- Attacks
  - Theft, demolition, changes in environment
  - Manipulation of hard-/software
- Counter measures
  - Tamper resistant devices, very difficult for sensors

“Over the Air”

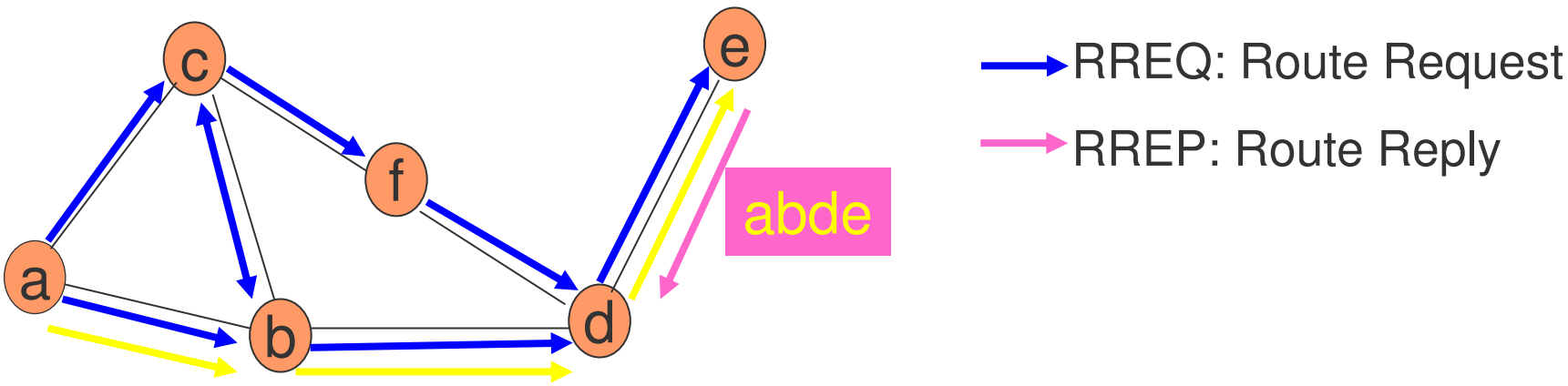
- Threats due to wireless communication
- Attacks
  - Eavesdropping, jamming, spoofing, “message attacks”
  - Sleep deprivation torture
- Counter measures
  - First attacks are not specific to ad hoc networks, well researched in military context:
    frequency hopping, spread spectrum

Collaboration

- Every algorithm in ad hoc networking depends on some extents from the collaboration of the other nodes
- Main example: Routing Protocols
  - Here: explaining the route discovery protocol

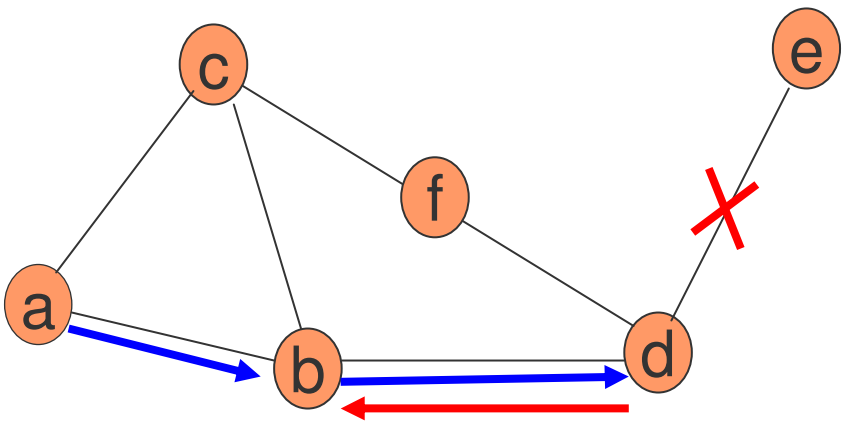
Route Discovery Protocol

- Used by DSR (Dynamic Source Routing)
- Simplified



Route Discovery Protocol (2)

- Behavior in case of error



RERR: Route Error

Route Discovery Protocol (3)

- Great number of attacks possible by
  - Not participating at all to save battery or partition the network
  - Spamming the network with RREQ
  - Changing routing information in RREP messages
  - Constantly or never replying with RERR
  - …

Solutions

- The CONFIDANT Protocol
  - Idea: punish non collaborative/malicious nodes by non-forwarding their traffic
  - Detection through “neighborhood watch”
  - Building a distributed system of reputation
  - Enable “re-socialization” through timeouts in the black list.

Sonja Buchegger, Jean-Yves Le Boudec: *Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks*. In Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing, Canary Islands, Spain, January 2002

Solutions (2)

- Nuglets
  - Idea: virtual currency to buy the collaboration
  - Nuglets are attached to the message
  - Each relaying node takes nuglets form the message which can use to buy the routing of its own message
  - Nuglet module must be implemented in a tamper resistant hardware to avoid cheating

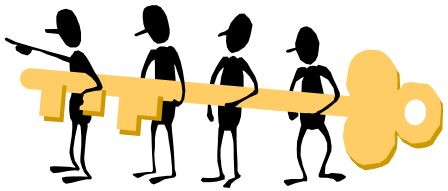
Jean-Pierre Hubaux, Levente Buttyan, Srdan Capkun: *The Quest for Security in Mobile Ad Hoc Networks*. In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Long Beach, CA, USA, October 2001

Solutions (3)

- Securing Routing Information
  - Idea: share the routing information through a secure channel
  - Requires Key Management and Security Mechanisms

Security Mechanisms

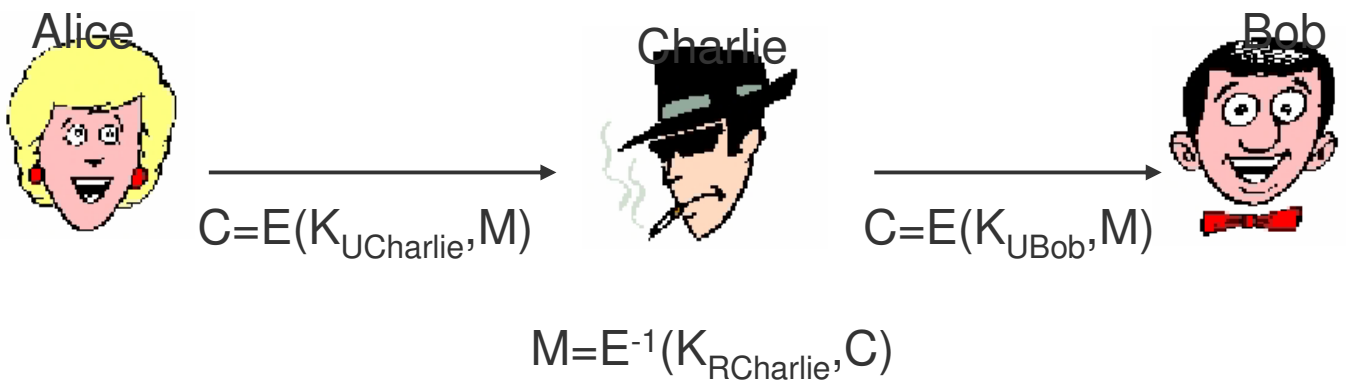
- Most critical and complex issue:
  Key Establishment
  - Key agreement
  - Key transport



- Asymmetric cryptography is appropriate for ad hoc networks to authenticate nodes

Asymmetric cryptography

- Each node has a public/private key pair
  - For efficiency reasons and to limit power consumption, use asymmetric cryptography to exchange symmetric keys, then use them to secure communication
- Threat: man-in-the-middle



Asymmetric cryptography

- How to authenticate the owner of a device?
- Classical solutions need a central trusted authority
  - Not suited for ad hoc networks

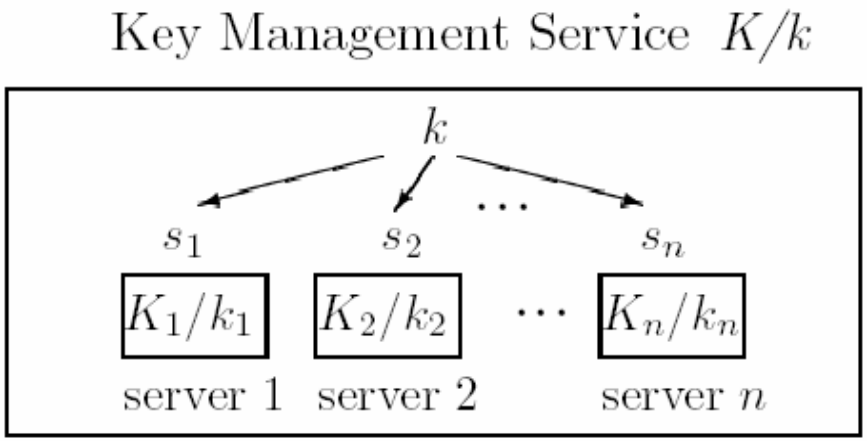
Resurrecting Duckling

- Ducklings emerging from their eggs
  - Recognize their mother as the first moving object emitting sound they see
- Similar approach for electronic devices
  - Recognize the owner as the first entity that sends a private key
- If the owner changes?
  - It should be possible to reinitialize the device (resurrect it)

Frank Stajano, Ross J. Anderson: *The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks*. In Proceedings of Security Protocols Workshop, 1999

Threshold cryptography

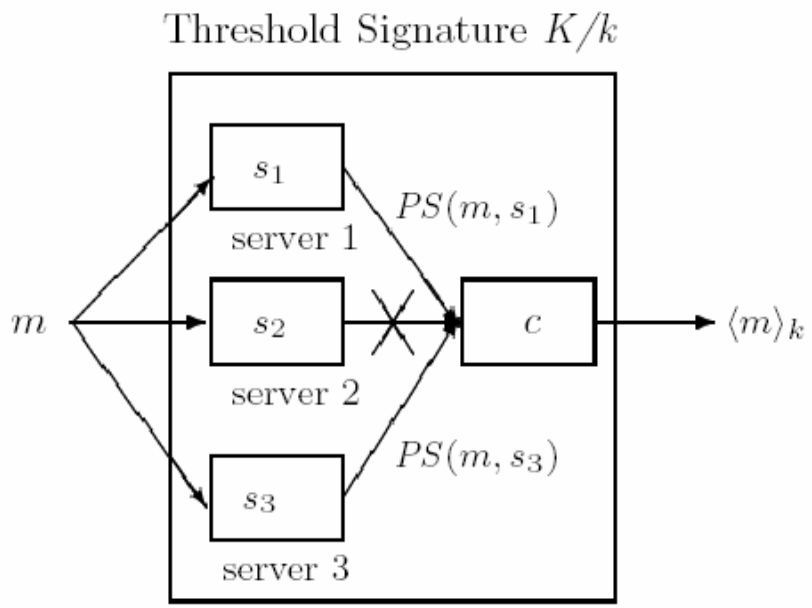
- Emulate the central authentication authority by distributing it on several nodes acting as servers
- Private Key is divided into n shares $s_1, s_2, \ldots s_n$



L. Zhou and Z. Haas: *Securing Ad Hoc Networks*. IEEE Network Magazine, vol. 13, no. 6, November/December 1999

Threshold cryptography (2)

- (*n*, *t+1*) threshold cryptography configuration
- *n* servers, if *t* are compromised, it is still possible to perform the service
- E.g. (3, 2) threshold cryptography scheme



L. Zhou and Z. Haas: *Securing Ad Hoc Networks*. IEEE Network Magazine, vol. 13, no. 6, November/December 1999

Threshold cryptography (3)

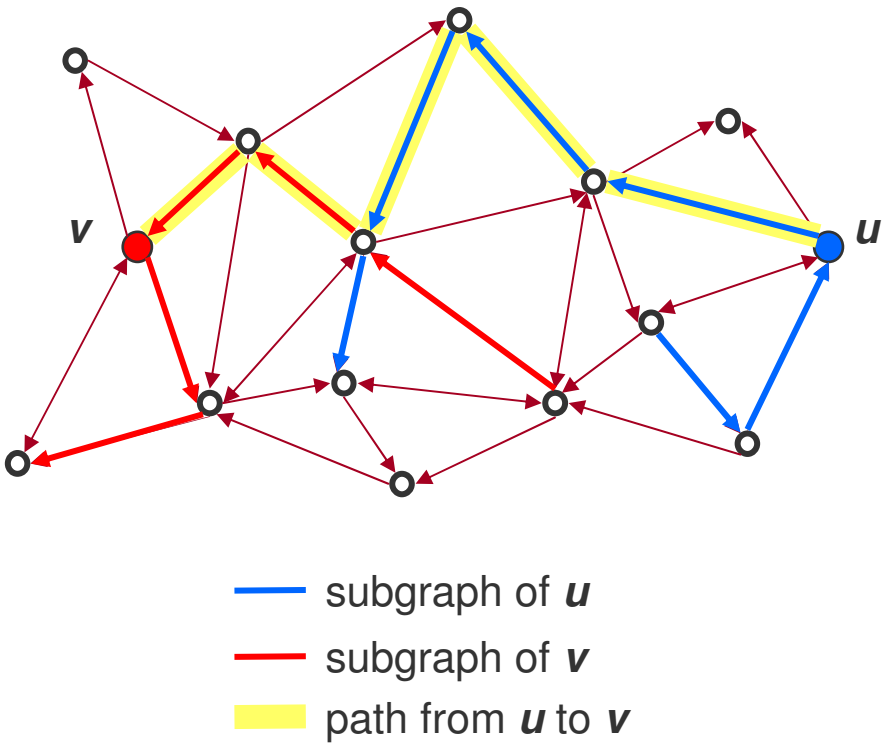
- Threshold cryptography seems to be a very robust solution
- However it needs some nodes to assume special behaviour
- For instance it is appropriate for military applications
- Inadequate for civilian networks
  - Users behave in a completely selfish way

Self-organized PKI

- Similar to PGP
- Certificate issued by users
  - Bind public key to an identity
- Each user maintains a local certificate repository
  - Certificates issued by itself
  - Other certificates selected using some algorithms (Shortcut Hunter)
  - Size of certificate repository is small compared to the total number of users in the system

Self-organized PKI (2)

- How it works
  - *u* wants to verify the public key of *v*
  - *u* and *v* merge their local certificate repositories (subgraphs)
  - *u* tries to find a certificate chain (path) from *u* to *v* in the merged repository



Jean-Pierre Hubaux, Levente Buttyan, Srdan Capkun: *The Quest for Security in Mobile Ad Hoc Networks*. In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Long Beach, CA, USA, October 2001

Self-organized PKI (3)

- Only probabilistic guarantee to find an appropriate certificate
- Security self-organized as the WWW?
  - How can these mechanisms be put in place preventing their misuse?

Common context

- The use of symmetric cryptography is also possible
- For the set up of an ad hoc network in case of a conference
  - Password could be written on a blackboard
- Idea: use another medium to exchange the keys

Conclusion

- Security in ad hoc networks is a very challenging issue
- Basic Mechanisms
  - Difficult to force the nodes to collaborate
  - No standard routing protocol yet

Conclusion (2)

- Because of their characteristics, ad hoc networks, are open especially to DoS attacks
- Classical security solutions are not suited for ad hoc networks
  - Security services should be distributed
- Standard protocols?
  - At the moment no universal solution

A Cooperative Security Scheme for Optimized Link State Routing in Mobile Ad-hoc Networks

João P. Vilela, João Barros

LIACC (Laboratory of Artificial Intelligence and Computer Science)

Faculdade de Ciências da Universidade do Porto

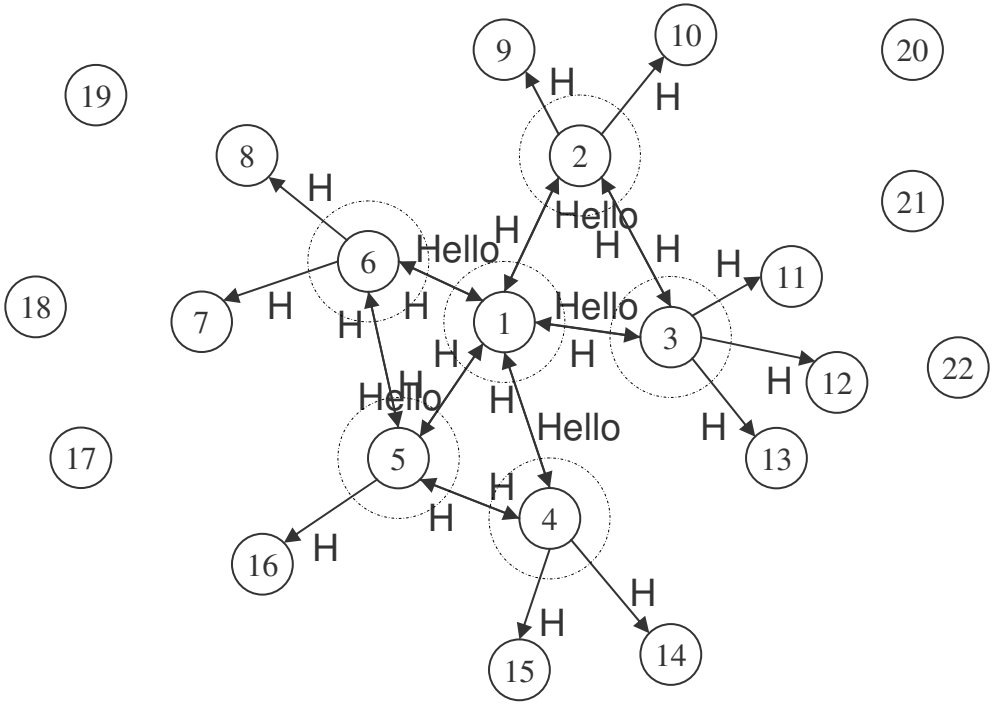
Outline

- Optimized Link State Routing (OLSR) protocol
  [Jacquet et al., 2001]
  - Overview
  - Security Issues
- Securing the OLSR protocol
  - Current Proposals
- Cooperative Security Scheme for OLSR
  - Description
  - Discussion
  - Evaluation
- Conclusions and Future Work

Optimized Link State Routing protocol

Overview

- Proactive, link state routing protocol
- Two types of control messages

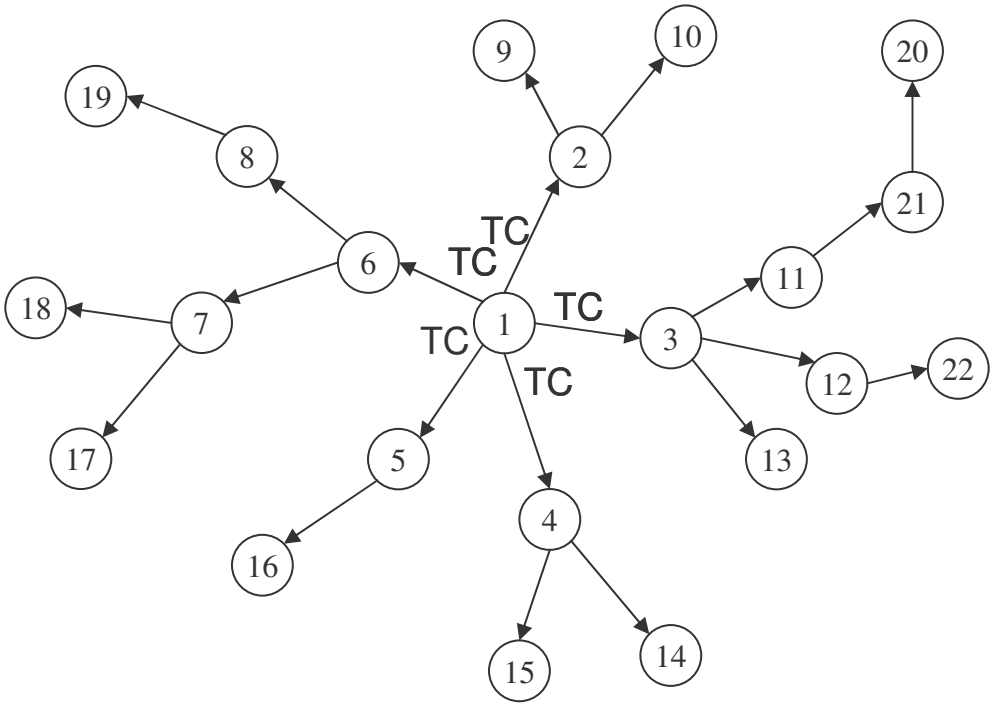


Hello messages:
-Between direct neighbors
-Info on neighbors up to two hops

Optimized Link State Routing protocol

Overview

- Proactive, link state routing protocol
- Two types of control messages



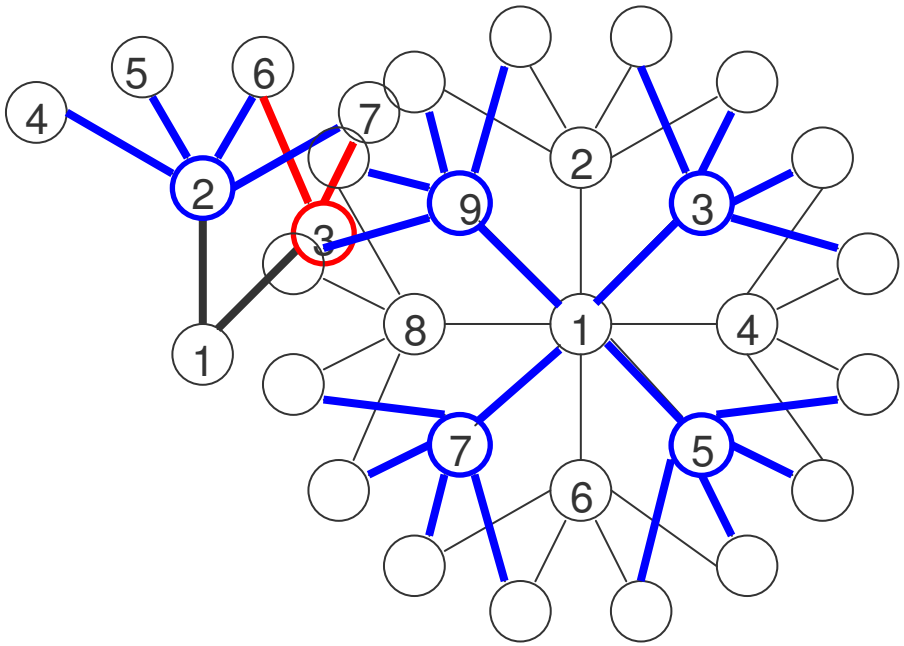
Hello messages:
-Between direct neighbors
-Info on neighbors up to two hops

Topology Control messages:
-Diffused to entire network
-Announce reachability to nodes

Optimized Link State Routing protocol

More than pure link state

- Simple, but effective optimization



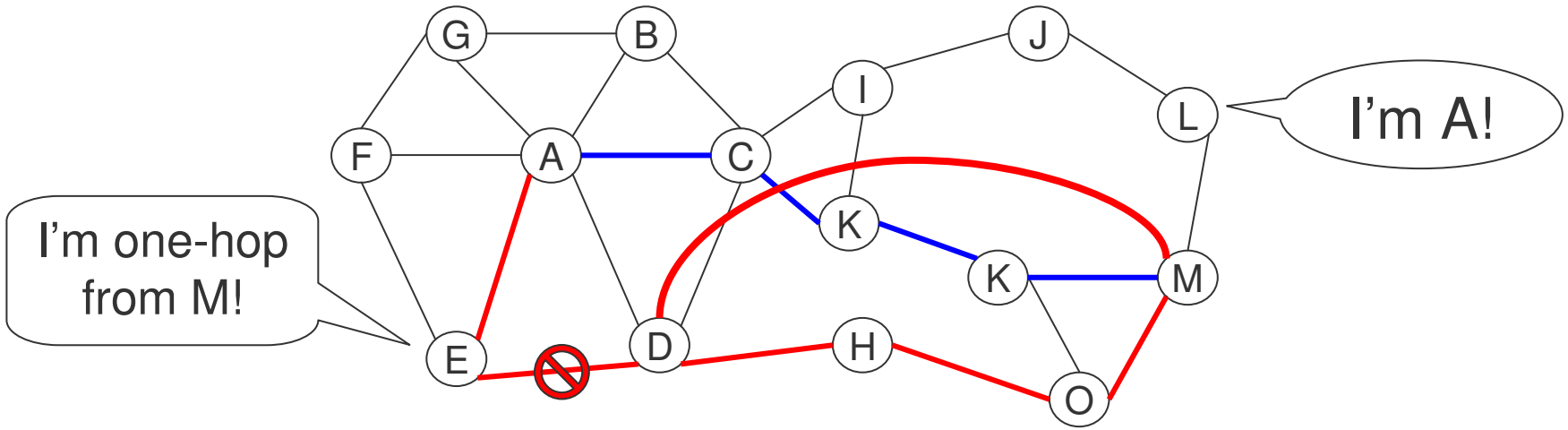
Multipoint Relays (MPR):
- subset of neighbors
- covers all two-hop
- all control traffic through MPRs

Gains:
- reduction of the amount of exchanged control traffic
- reduction of the size of control messages

Optimized Link State Routing protocol

Security Issues

	Description/Scenario	Result
Identity spoofing	Generation of messages pretending to be another node	Conflicting routes to the node being spoofed
Link spoofing	Generation of messages announcing reachability to an unreachable node	Traffic interception; Increase of path lengths
Traffic relay / generation refusal	Refuse to generate its own and to relay control traffic of other nodes	Loss of connectivity; Degradation of communications
Replay attack	Resend previously sent (authenticated) messages	Outdating and/or conflicting information into the network
Wormhole attack	Two nodes collude and exchange encapsulated packets	Traffic interception; Increase of path lengths

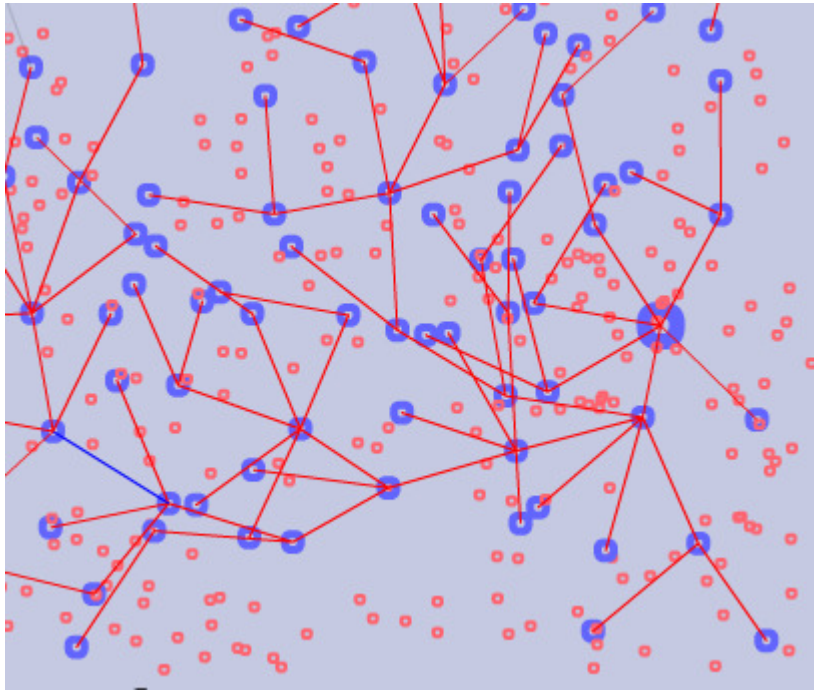


Securing the OLSR protocol

Current Proposals

	Proposed Solution
Identity spoofing	Cryptographic signatures with each message [Raffo et al.] ✓
Replay attack	Timestamp messages [Adjih et al.] ✓
Link spoofing	?
Traffic relay / generation refusal	Geographical positioning [Adjih et al.] Packet counting technique [Adjih et al.] ?
Wormhole attack	?

A Cooperative Security Scheme for the Optimized Link State Routing protocol



"MPR Flooding"
Source: INRIA Project HIPERCOM OLSR webpage

Cooperative Security Scheme for OLSR

Description

- Goal: assure that nodes correctly generate and relay control traffic
- Assumption: key management infrastructure
- Combination of two sources of traffic information:
  - The (unreliable) monitoring of packet relays [Marti et al.]
  - The paths traversed by successfully delivered packets
- Three new elements:
  - Complete path message (CPM)
  - Rating table
  - Warning message

Cooperative Security Scheme for OLSR

Specification

1. When a HELLO is received, the source node is added to the Rating Table;

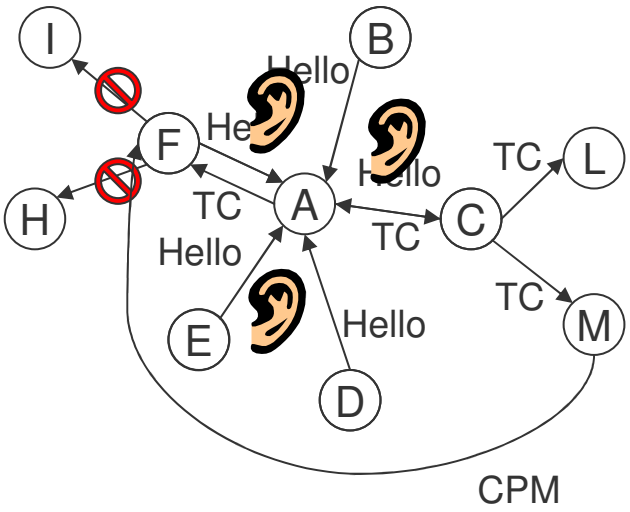
2. If a message is sent and retransmitted, the secondary rating is increased and decreased otherwise;

3. When a TC is successfully received, the path traversed is sent back on a CPM with a certain rate;

4. If the path in the CPM is consistent with the information announced by neighbors:

    1. Increase the primary rating if the secondary rating is higher;
    2. Decrease the primary rating otherwise.

Node	Primary	Secondary
B	α	ρ
C	α	ρ
D	α	ρ
E	α	ρ
F	α	ρ



Cooperative Security Scheme for OLSR

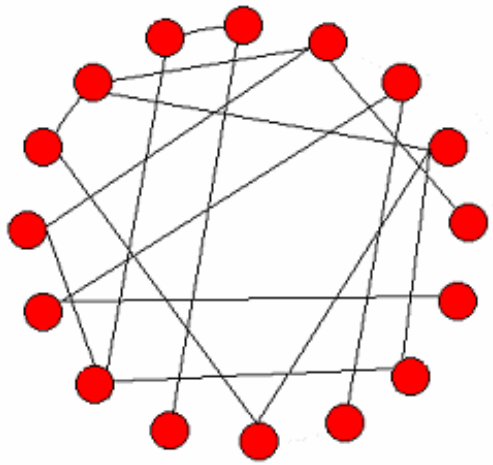
Discussion

- Punish nodes accordingly to their primary rating
- Link spoofing results in degradation of communications to the malicious node
- Traffic relay/generation refusal can be detected by a correlation of the number of CPMs received and the density of the network
- Identity spoofing and replay attacks are solved by a key management system and timestamps

Cooperative Security Scheme for OLSR

Evaluation – Control traffic overhead

- In terms of IP addresses transmitted
- Random Graph Model (N nodes, link probability p)
  - Plain link-state: $O(N^3)$
  - OLSR: $O(N (\log N)^2)$
  - CSS-OLSR: $O(N (\log N)^2)$
- Random Unit Graph (N nodes, unit length L)
  - 1D
    - Plain link-state: $O(N^3 / L)$ (from TCs)
    - OLSR: $O(N^2 / L)$ (from HELLOs)
    - CSS-OLSR: $O(N^2 / L)$ (from HELLOs)
  - 2D
    - Plain link-state: $O(N^3 / L^2)$ (from TCs)
    - OLSR: $O(N^2 / L)$ (from HELLOs)
    - CSS-OLSR: $O(N^2 / L)$ (from HELLOs)



Conclusions and Future Work

- Doing:
  - Implementing and testing through simulation
  - Fine tuning the protocol parameters
- Following steps:
  - Integrate the MPR selection with the rating table and the key management infrastructure
  - Determine the long-term convergence of the protocol using a game theoretic analysis